(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 November 2001 (01.11.2001)

PCT

(10) International Publication Number
WO 01/82190 A1

(51) International Patent Classification[7]: G06F 17/60, 11/30, H04L 9/00

(21) International Application Number: PCT/US01/13232

(22) International Filing Date: 25 April 2001 (25.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/558,898 26 April 2000 (26.04.2000) US

(71) Applicant *(for all designated States except US)*: **GLOBAL TRANSACTION COMPANY** [US/US]; 505 King Avenue, Columbus, OH 43201 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **RENNER, George, Frederick** [US/US]; Residence: Dublin, Ohio, c/o 505 King Avenue, Columbus, OH 43201 (US).

(74) Agent: **BARANOWSKI, Edwin, M.**; Porter, Wright, Morris & Arthur LLP, 41 South High Street, Columbus, OH 43215 (US).

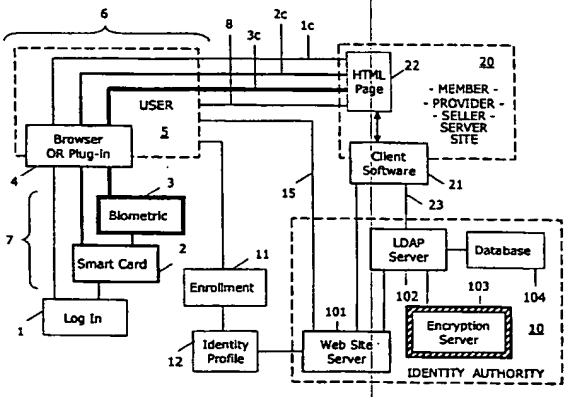
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

[Continued on next page]

(54) Title: MULTI-TIERED IDENTITY VERIFICATION AUTHORITY FOR E-COMMERCE



(57) Abstract: Any single or combination of password log-in (1), mart card (2) or biometric (3) identification routines may be adapted in the system by authority software (4) used in conjunction with the user's browser and/or terminal (5). The ID authority (10) is interconnected between an enrolled user (6) and web site provider (20) and controls enrollment, customer support and administration. The ID authority site (10) includes interconnected web site server (101), LDAP server (102), encryption services server (103) and database (104) containing user and subscriber profiles. Web site providers (20) subscribing to the ID authority (10) includes identity verification software scripts provided by the authority (10) in their HTML pages (22). Communications between the user (5) and ID authority (10) may be encrypted through server (103). The identity data from the user (5) in compliance with the demand is sent in a message packet (15) to the authority (10). Depending on the comparison result, a response is sent, either failure or success is sent to the user terminal (15). The user terminal (15) then transmits the verification code (23) to the identity authority (10). In enrolling in the system (11), the user (5) provides an identity profile (12) that can include a combination of biometrics and authentication methods (1c), (2c), or (3c). The biometric software (7) is installed on the user terminal (15). The browser software includes a mechanism for conventionally communicating with a web site and for receiving a verification demand from a web site (8).

WO 01/82190 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

MULTI-TIERED IDENTITY VERIFICATION AUTHORITY FOR E-COMMERCE

FIELD OF THE INVENTION

This invention relates to e-commerce, particularly, a mechanism and system for third party verification of the identity of Web and Internet commerce participants, and other participants in Web information transactions and communications ("e-commerce"), namely, an identity authority ("ID Authority") that is useful with Web and other Internet sites and their users as an improvement of the next generation of Internet infrastructure.

BACKGROUND AND SUMMARY OF THE INVENTION

In electronic commerce business using the World Wide Web and the Internet, there is a need for better proof of a customer's identity than is provided currently by password login. Most Web users also desire a more secure and convenient way to identify themselves for Web transactions. Financial institutions, pharmaceuticals distributors, and retailers are among the groups that would benefit from improved identity verification mechanisms.

It is an object of the invention to provide a service mechanism and system to act as a third party to verify identity for e-commerce participants using passwords, smart cards, and biometrics in a hierarchy, and combinations thereof depending on the need for security. The service will verify the identity of a person using a Web browser and allow that user to interact with the Web site or other Internet mechanism. The system can also verify the Web site to the user, and optionally, the personal identity of an individual user at the Web site. As a further option, the service can verify the personal identities of two Web participants to each other.

It is a further object to allow verifications to be requested at more that one level, instance by instance: a lower-risk action may only need smart card verification; a high-risk transaction may require biometric verification; or intermediate levels may be provided. Users are able to opt for one or more different levels of participation, with higher levels allowing them to meet requests for higher-level verifications. The invention is intended to benefit participants by removing the complexity of implementing and administering unique trust relationships while achieving the benefits of verified identity in electronic communications and transactions.

It is an object of the invention to substitute for and provide analogous functions to the Certificate Authority function in the current Public Key Infrastructure (PKI) identification mechanisms. It is also an object of the invention to provide third-party network directory services integrated with the identity verification authority service.

The invention is described more fully in the following description of the preferred embodiment considered in view of the drawings in which:

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 shows the prior art structure in which each user requires a separate and unique relationship with every other user. Every time a new user is added to the population, every member needs to add a new relationship.

Figure 2 illustrates the identity authority mechanism and system in which adding a new user involves adding only one relationship with an identity authority. The benefits of the authority mechanism and system compound as the populations of Web sites and users grow.

Figure 3 shows system architecture and identity authority structures, relationships and operations in the preferred embodiment.

DETAILED DESCRIPTION OF THE INVENTION AND THE PREFERRED EMBODIMENT

In the mechanism and system of the invention, each user will receive a kit including a smart card, a smart card reader and biometric reader, or combined reader. A lower-price option may be a smart card reader only. Installation software to install the readers and identity verification system of the invention for use in conjunction with a Web browser is also provided. The software may be stand alone for exclusive use with the system or may be provided in the user kit as a plug-in for an OEM browser such as Microsoft Explorer® or Netscape Navigator®. Each member / client Web site or participating Internet site will implement scripts in their Web content HTML pages as explained below to make use of the identity authority mechanism and directory system.

In an example, from the user's perspective, a corporate buyer deals with different Web marketplaces for office supplies, financial services, construction, energy and maintenance, and other new areas that are added frequently. If each of these marketplaces has its own (and likely unique) method for validating identity and "signing" a transaction, as shown in Figure 1, each buyer or user, U1 – Un, will require considerable physical and intellectual overhead to maintain encrypted passwords and the like that are necessary for an entry relationship to all seller, S1 – Sn, web sites. If, on the other hand, the marketplaces referred the identity verification function to the authority mechanism and system of the invention as shown in Figure 2, each buyer or user would need only one set of credentials maintained by the Identity Authority with regard to users and sellers. Each marketplace operator would be relieved from the burden of maintaining a

verification infrastructure in instances when identity verification is required in e-commerce.

The mechanism and system is useful with many categories of participants in Internet transactions, in addition to business transactions that depend on certification of an individual's identity. One example of such a transaction is the Federal government mandate that electronic benefits enrollments and renewals be validated using a biometric verification of identity. Other examples are the regulatory mandates in California and Ohio that online drug prescriptions must have a biometric or other certification of the prescribing doctor's identity. Similarly, many other large examples, such as B2B ("business-to-business") contracting and banking, may not have a government mandate but do have the interests of the participants in reducing fraud and liability exposure.

The invention is also useful to small companies currently facing problems of recognition on the Web. The identity verification authority mechanism and system of the invention assists business on the Web by backing their presence. In B2B commerce that by 2002 is estimated to grow to nearly 75% of corporate buyers and sellers doing over $750 billion in transactions, the invention is likewise useful. The low cost and many-to-many Internet connectivity is motivating businesses to migrate in whole or in part to Web and Internet marketplaces from the Old Economy one-to-one relationships. This commercial movement, however, also creates new openings for misrepresentation and fraud. The biometric identity verification mechanism and system enhances individual accountability onto the Web.

In the preferred embodiment, a signup fee and annual renewal per user are charged to the user organizations and a transaction fee per verification is charged to the Web site seller or other provider.

In its full multi-layer function, the invention will complement, or support, current public key encryption (PKI) certifications of authenticity (CA's) such as VeriSign® and CyberTrust®. Legacy institutions, such as banks, and the USPS will find the invention readily adaptable to their use in view of the fact that many banks have limited technical resources. Large membership sites such as AOL®, and Yahoo® are configured for a very large population of loosely-held consumer relationships. To perform an authority service, such sites would need to change their business model. Such types of sites, however, have access to corporate relationships and technical resources through and by which the invention may be implemented.

With regard to partial function identification without biometrics, public key CA's can promote the use of PKI mechanism and systems to fill a digital signature role, and implement a mechanism to make PK certificates portable using smart cards or other means. Private PKI implementations using proprietary software can fill the role in closed communities. In further applications, Web logon identity managers such as eCode.com®, Ezlogin.com®, and Digitalme® may adapt operations to the smart card and biometric roles, in the context of large numbers of loose relationships.

The nature of the identity authority mechanism and system is indifferent to differences between business users and consumer users; the preferred embodiment favors a business orientation in which a population of users and a group of Web sites using the mechanism and system are quickly established in a

group of Web site operators that serve a shared user population. Online auctions are an example. Since these marketplaces are often established by a business that wants to operate the auction site, these operating auction companies are points of entry for the market. In implementing the authority mechanism and system at multiple auction operators efficiencies of simplicity and economy as depicted in Figure 2 can be achieved. Web based pharmacies, MD's, banks and Web marketplaces are also potential users.

The system provides from the standpoint of a user, a simplified and direct mechanism for standardized user verification. From the standpoint of the site provider, the system offers convenience to users and adds a mechanism whereby access, purchase and other site functions can be predeterminedly controlled in accordance with specific rules and criteria related to individual users and transactions.

In its general description, the system includes a user kit consisting of a smart card, a smart card reader and biometric reader, or combination, and software for the user's terminal, usually a PC, and browser. A lower-priced variant may omit biometric capability. These components are available as semi-custom or off-the-shelf products. On the Web provider side, the invention provides a mechanism and system that verifies identification packets sent by the seller's Web server, assembled from a combination of off-the-shelf products and custom software, in addition to the existing back room implementation. The user kit enables the establishment of a user identity profile interrelated among the categories of log-in, smart card and biometric routines. For example, the smart card may include a fingerprint profile that will be compared in the identification process at the user terminal to the reading created by the biometric reader.

Alternatively or additionally, the fingerprint profile may be maintained in the remote ID Authority database for comparison.

The system acts as a third party in Internet interactions, including but not limited to HTTP (Web), e-mail, FTP, WAP, etc., to verify personal identity. Optionally other information such as corporate affiliations and authorizations of one participant to the other and personal identities and other information of participants are verified to each other. One version, specific to a World Wide Web use of the invention, employs a sequence of operations as follows:

EXAMPLE I

1. The ID Authority business enters an agreement with a Web business site to provide the identity verification function. The Web site adds specific software scripts to their HTML pages wherever the identity verification functions are needed.

2. A business Web user is enrolled in the identity verification service and receives a user kit containing software components, a smart card reader, and a biometric reader to install on their PC, and a personalized smart card.

3. To begin a particular interaction, the user browses to the Web site and to the particular page of interest. The Web site downloads a page containing the scripts to use the identity verification service.

4. The script in the Web page executes on the user's PC, making use of the software components installed from the user kit to collect the claimed identity plus evidence to support that claim;

specifically to access and manipulate the smart card and biometric reader if those options are being used. The software components generate a message packet to the identity authority containing the claimed identity and the evidence to support that identity.

5. The identity authority examines the evidence provided in the packet and generates a response. If the comparison fails, the response contains only a failure notification. If the comparison succeeds, the response contains a success notification and a unique verification code. The response is sent to the user's PC.

6. The scripts continuing to execute in the user's PC handle the response, placing the verification code and positive response in their positions in the requesting page. Either upon receipt or on user action, the request page with the appropriate data items is dispatched to the Web server. Either immediately or later, depending on business needs, the Web server can send a message packet to the identity authority requesting a check of the verification code returned by the user. The reply to this request will be a simple Yes/No depending on the results of the check plus any requested optional information such as authorizations.

The above methods may be adapted to use cryptography-based methods to verify identity. In a variation, the system uses smart card based methods, optionally in combination with cryptography methods, to verify identity and provide other optional information. In this variation, the software components on the users PC would interact with the smart card to produce data elements, and

optionally, a cryptographic Message Authentication Code (MAC) for a message to the requesting participant. That participant could then submit the message to the ID Authority for verification.

Biometric methods are optionally used in combination with smart cards and cryptography to verify identity in the preferred embodiment. A version adapted to World Wide Web use follows:

EXAMPLE II

1. The ID Authority business enters an agreement with a Web business site to provide the identity verification function. The Web site adds specific software scripts to their HTML pages wherever the identity verification functions are needed.

2. A business Web user is enrolled in the identity verification service and receives a user kit containing software components, a smart card reader, and a biometric reader to install on their PC, and a personalized smart card.

3. To begin a particular interaction, the user browses to the Web site and to the particular page of interest. The Web site downloads a page containing the scripts to use the identity verification service.

4. The script in the Web page executes on the user's PC, making use of the software components installed from the user kit to collect the claimed identity plus evidence to support that claim; specifically to access and manipulate the smart card and biometric reader. The software components: (a) retrieve the claimed

identification and primary biometric template from the smart card after satisfying the smart card file access methods; (b) read a live fingerprint from the user, prompting if necessary; (c) match the live fingerprint to the template and generate a verification message packet containing the claimed identity, the results of the match, a timestamp and transaction sequence number, and a MAC generated by the smart card; and (d) return the identification data, indication of biometric match, and the verification message packet to the calling script.

5. The scripts continuing to execute in the user's PC handle the response, placing the data elements in their positions in the requesting page. Either upon receipt or on user action, the request page with the appropriate data items is dispatched to the Web server.

6. Either immediately or later, depending on business needs, the Web server can send the verification message packet to the identity authority requesting a check of the MAC returned by the user. The identity authority recalculates the MAC, compares it to the value provided in the packet, and generates a response. If the comparison fails, the response to the Web server contains only a failure notification. If the comparison succeeds, the response contains a success notification and a unique verification code.

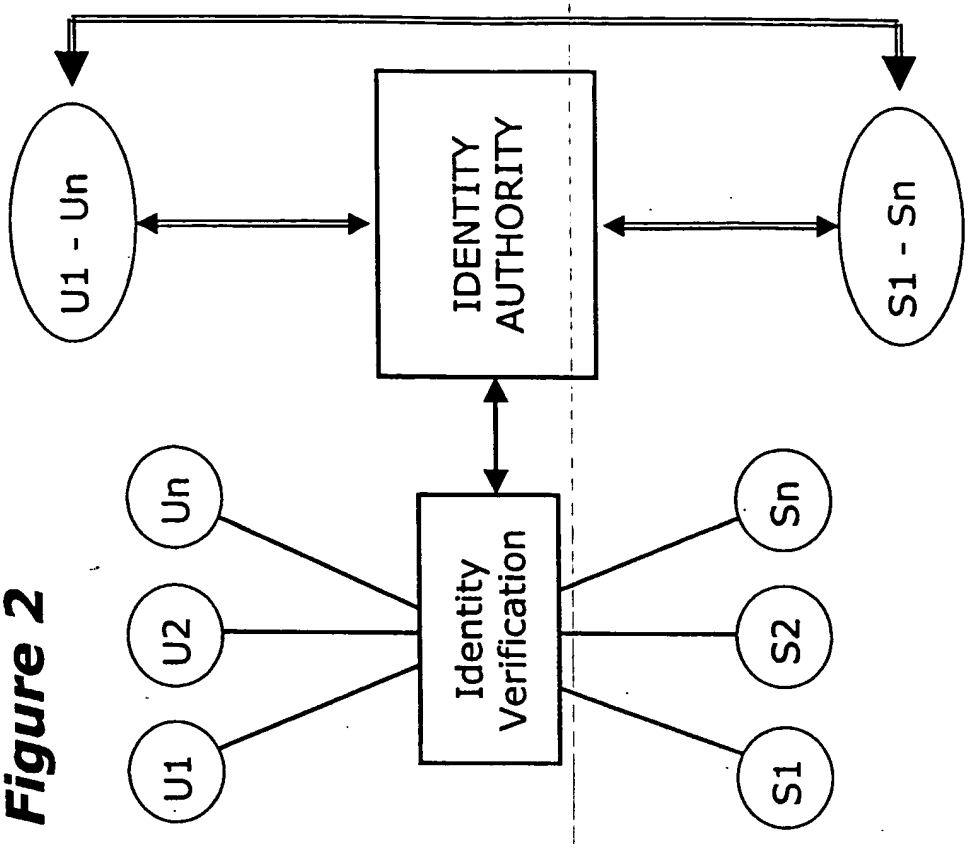
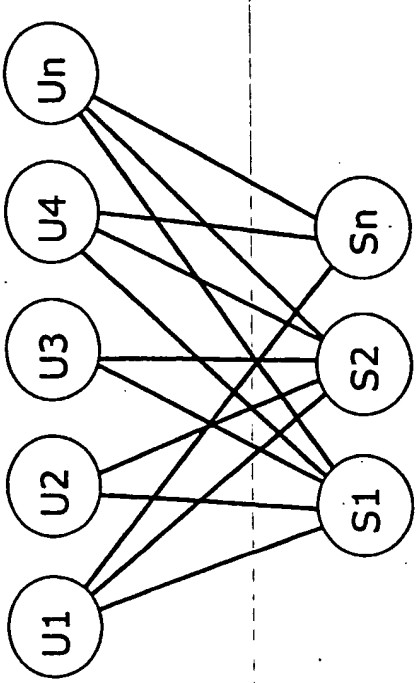


Figure 2



Prior art

Figure 1

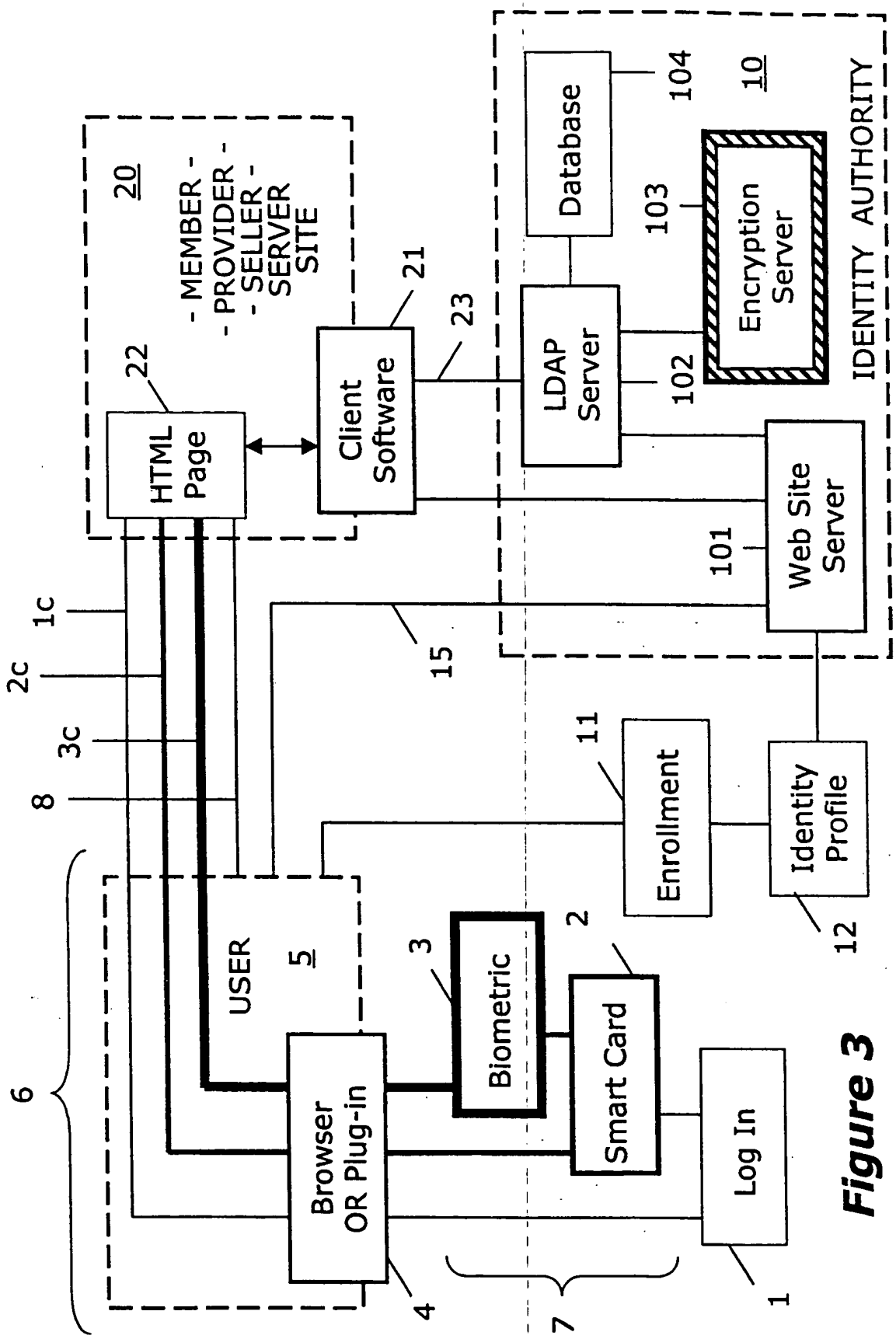


Figure 3

BEST AVAILABLE COPY

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/13232

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : GO6F 17/60; 11/30; HO4L 9/00
US CL : 705/26, 705/42, 705/43, 713/155, 713/164, 713/165, 713/166, 713/186, 713/200, 713/201
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 705/26, 705/42, 705/43, 713/155, 713/164, 713/165, 713/166, 713/186, 713/200, 713/201

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
N/A

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
East and Dialog Search; identity or certified or certifying or verification or verified adj authority, web or internet adj service adj provider, biometries

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y,P	US 6,212,634 B1 (Geer, Jr. et al.) 03 April 2001, see col. 2 lines 57-67, col. 3 lines 1-41, col. 6 lines 58-67, and col. 9 lines 19-66.	1, 2, 3, 7, 9
Y,P	US 6,182,076 B1 (Yu et al.) 30 January 2001, see col. 5 lines 13-17 and 45-47, col. 7 lines 20-29, col. 8 lines 10-17, col. 9 lines 12-18, and col. 10 lines 10-61.	1, 3, 7, 8, 9, 12
Y,P	US 5,987,232 A (Tabuki) 16 November 1999, see col 4 lines 29-43 and 61-67, col. 7 lines 42-61.	1, 7, 8
Y,P	EP 0935221 A2 (Hiroshi Nakamura et al.) 08 November 1999, see col. 4 lines 1-49, col. 5 lines 34-50-58, and col. 6 lines 1-21.	1, 7, 8
A	US 5, 615, 268 A (Bisbee et al.) 25 March 1997, see col. 4 lines 1-26, and col. 5 lines 16-54.	1

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 July 2001 (24.07.2001)	31 AUG 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Gail Hayes James R. Matthews Telephone No. (703) 306-0426

Form PCT/ISA/210 (second sheet) (July 1998)

Thus, it can be seen that the system offers participants case-by-case options on the level of identity verification to be required for Internet interaction. For example, a Web site could require only smart card methods for simple log-in but require a biometric verification to complete purchases over some threshold level of dollar value or other risk metric.

In its implementation, the system may provide services integrated with a P3P implementation for negotiating one participant's access to the other participant's identification and other information. The services may be integrated with a database, X.500, or other directory implementation accessed using LDAP, DAP, or any database access protocol. A version for LDAP implementation follows:

EXAMPLE III

1. The ID Authority business enters an agreement with a Web business site to provide the identity verification function. The Web site adds specific software scripts to their HTML pages wherever the identity verification functions are needed.

2. A business Web user is enrolled in the identity verification service and receives a user kit containing software components, a smart card reader, and a biometric reader to install on their PC, and a personalized smart card.

3. To begin a particular interaction, the user browses to the Web site. The Web server returns a login request page containing the scripts to use the identity verification service.

4. The script in the Web page executes on the user's PC, making use of the software components installed from the user kit to collect the claimed identity plus evidence to support that claim, specifically to access and manipulate the smart card and biometric reader if those options are being used. The software components generate data elements containing the claimed identity and the evidence to support that identity.

5. The scripts continuing to execute in the user's PC place the data elements in their positions in the login request page. Either upon receipt or on user action, the log-in request with the appropriate data items is dispatched to the Web server. As a part of processing the login request the Web server assembles an LDAP call containing the data elements and dispatches it to the ID Authority LDAP server. The ID Authority server verifies identity and places the results of the verification, plus any other related authorization data, in the LDAP response message.

With reference to Figure 3 showing the system architecture, any single or combination of password log-in 1, smart card 2, or biometric 3 identification routines may be adapted in the system by authority software 4 used in conjunction with the user's browser and/or terminal 5. The ID Authority will be identified as an icon on client Web pages that will also include a brief dialog for functions. The ID authority 10 is interconnected between an enrolled user 6 and web site provider 20 and controls enrollment, customer support and

administration. The ID authority site includes interconnected web site server 101, LDAP server 102, encryption services server 103 and database 104 containing user and subscriber profiles. Web site providers subscribing to the ID authority include identity verification software scripts provided by the authority in their HTML pages 22.

In enrolling in the system 11, the user provides an identity profile, such as user name and password, smart card identification code, and a biometric indicia such as a fingerprint read compiled in a data file 12 maintained by the authority at site database 104. The user kit providing password log-in and smart card reader and biometric reader hardware for higher levels of authentication and authority software 7 is installed on the user terminal. As noted the software may be a plug-in for an OEM browser or a custom browser with ID authority functions integrally included. The user kit components are operatively interconnected with browser 5. The user is also provided with a personalized smart card (not shown) for operative relationship with the reader. The browser software includes a mechanism for conventionally communicating with a web site and for receiving a verification demand from a web site 8.

When the web site is an identity authority subscriber 20, the site prompts the user to comply with an identity demand when verification scripts in the web site HTML page 22 initiate an interaction between the user and the web site by downloading to the user's browser a verification script initiating the identity verification process. The downloaded verification script executes on the user's terminal and signals the user that a verification is required in one or more than one of the forms of a user name and password, a smart card identity, and a biometric identity, or a combination thereof. Upon receipt, the browser

mechanism prompts the user to comply with the demand, to provide identity data from the user in compliance with the demand, and to send a message packet to the authority containing the collected identity data. Communications between the user and ID Authority and the ID Authority may be encrypted, for example through server 103. The identity data from the user in compliance with the demand is sent in a message packet 15 to the authority.

Examples of ID Authority functions are included in Table 1 below:

TABLE 1

Function	Query / Demand	Response
Identification	Who are you?	I am Doug James.
Verified Identification	Who are you?	I am Doug James. My verification code is 3a665mn48277db#346& ....
Verified Transaction Signature	Who are you? Who is really purchasing this lot of pharmaceuticals? What is your authority?	I am Doug James. Doug James is agreeing to this transaction for XYZ Corp. My ID Authority verification code is 6593vz748d4827d% ....

In the order of relative importance and security needed for the transaction used as an example in the table above, the tiered verification functions of identification, verified identification, and verified transaction signature may correspond to password log-in, smart card verification and biometric (*eg.* fingerprint) identification demands.

In the verification process, the signal of the web site to the user that a verification is required in one or more than one of the forms of a user name and password, a smart card identity, and a biometric identity is predetermined at the web site depending on the relative need for certainty of an identity verification related to the degree of importance of the electronic commerce to be transacted.

The identity authority compares the data in the packet sent from the user with the user identity profile data 12 maintained by the authority in its database 104. Depending on the comparison result, a response which is either a failure notification, or a success notification and a unique verification code, is sent to the user terminal 15 for transmission to the web site. The user terminal then transmits 8 the verification code to the requesting web site page, which then transmits the code 23 to the identity authority for authentication that the code provided is in fact the code sent to the user by the ID Authority. The ID Authority will either approve, or disapprove, the user identity. With approval secure identity verified communications between the user and web site may proceed consistent with the level of identification, 1c, 2c or 3c, required and consistent with predetermined identity authorization activities allowed to the particular user. For example, some users, although their identity may be sufficiently verified may not have authority to make purchases, or to make purchases in excess of a given value, or to access certain information.

Having thus described the invention in detail, those skilled in the art will appreciate that, given the present disclosure, modifications may be made to the invention without departing from the spirit of the inventive concept herein described. Therefore, it is not intended that the scope of the invention be limited to the specific and preferred embodiments illustrations and described. Rather, it is intended that the scope of the invention be determined by the appended claims.

<<< † >>>

WHAT IS CLAIMED IS:

1. A multi-tiered identity verification authority system for e-commercecomprising:

an identity authority interconnected between an enrolled user and member Internet or Web site providers, the site providers subscribing to the authority and including identity verification software scripts provided by the authority in their HTML pages, the user having enrolled and provided identity data maintained by the authority;

a user kit installed on a user terminal including a browser having identity verification functions and at least one of a smart card reader and a biometric reader operatively interconnected with the browser, and a personalized smart card, the browser including a mechanism for receiving a verification demand from a site, for prompting the user to comply with the demand, for collecting identity data from the user in compliance with the demand, and for sending in a message packet to the authority the collected identity data;

the verification scripts in the site HTML page including means to begin an interaction between the user and the site by downloading to the user's browser a verification script initiating an identity verification;

the downloaded verification script executing on the user's terminal signaling the user that a verification is required in one or more than one of the forms of a user name and password, a smart card identity, and a biometric identity and, upon receipt, initiating the browser mechanism to prompt the user to comply with the demand, to collect identity data from the user in compliance with the demand, and to send a message packet to the authority containing the collected identity data;

the identity authority comparing the data in the packet with a user identity profile in a database maintained by the authority and generating a response which is

either a failure notification or a success notification and a unique verification code depending on the comparison and sending the response to the user terminal for transmission to the site;

means in the user terminal for transmitting the verification code to the requesting site page whereby the web page server transmits the verification code to the identity authority for an authentication approval or disapproval that is transmitted back to the site that permits or denies user access to the website.

2. The verification authority of claim 1 including a smart card file access protocol.

3. The verification authority of claim 2 further including interconnected mechanisms at the user terminal whereby upon receipt by the user terminal of an identity demand, the user terminal retrieves a demanded identification and biometric template from the smart card.

4. The verification authority of claim 3 in which a demand for a biometric identification results in a prompt at the user terminal that the user provide a fingerprint.

5. The verification authority of claim 4 in which a user provided fingerprint is compared to the fingerprint of the smart card template.

6. The verification authority of claim 5 in which the identity message packet returned to the authority from the user terminal includes a timestamp and transaction sequence number.

7. The verification authority of claim 1 in which the authority includes a database of identity profiles of enrolled users with regard to verification criteria and in processing the login request from the site page, the web server assembles an data base access protocol call containing the data elements demanded and dispatches it to the authority database server.

8. The verification authority of claim 7 in which in the verification process, the identity authority data base server places the results of the verification, and other related authorization data, in the data base access protocol response message.

9. The verification authority of claim 1 in which in the verification process, the signal of the site to the user that a verification is required in one or more than one of the forms of a user name and password, a smart card identity, and a biometric identity is predetermined at the site depending on the relative need for certainty of an identity verification related to the degree of importance of the electronic commerce to be transacted.

10. The verification authority of claim 1 in which the user kit includes a plug-in for an OEM browser.

11. The verification authority of claim 1 in which the authority response includes a time stamp and a cryptographic message authentication code.

12. A user kit for the multi-tiered identity verification authority system of claim 1 comprising a smart card, a smart card reader, a biometric reader and a browser plug-in.